Deployment Guide

Release 2305 – May 2023

cxAddOns

Global AddOn specialist for Enterprise Software.

1 SYSTEM LANDSCAPE 3

2 EXCHANGE SETUP 4

2.1 ACTIVATE EWS AND LOCAL AUTHENTICATION 4

2.1.1 Local Exchange Server 4

2.1.2 Office 365 4

2.2 SETUP MAILBOX ACCESS 4

2.2.1 Dedicated Service User 4

2.2.1.1 Rights on mailbox-database-level 5

2.2.1.2 Allocation of rights via RBAC role 5

2.2.1.3 Individual Access to Mailboxes 6

2.2.2 Authorization via OAuth (Office 365) 10

2.2.3 NOTE ABOUT THE AZURE API PERMISSIONS 19

2.3 EXCHANGE THROTTLING POLICY 20

2.4 CONNECTION BETWEEN EXCHANGE AND SAP BUSINESS TECHNOLOGY PLATFORM (BTP) 21

3 SAP SALES CLOUD SETTINGS 23

3.1 WEBSERVICES 23

3.2 BUSINESS CONFIGURATION 23

3.3 COMMUNICATION USER 24

3.4 SETUP COMMUNICATION SCENARIOS 28

3.4.1 Communication System 28

3.4.2 Communication Arrangements 29

3.5 EVENT NOTIFICATIONS 30

3.6 CREATE RELATIONTYPE 33

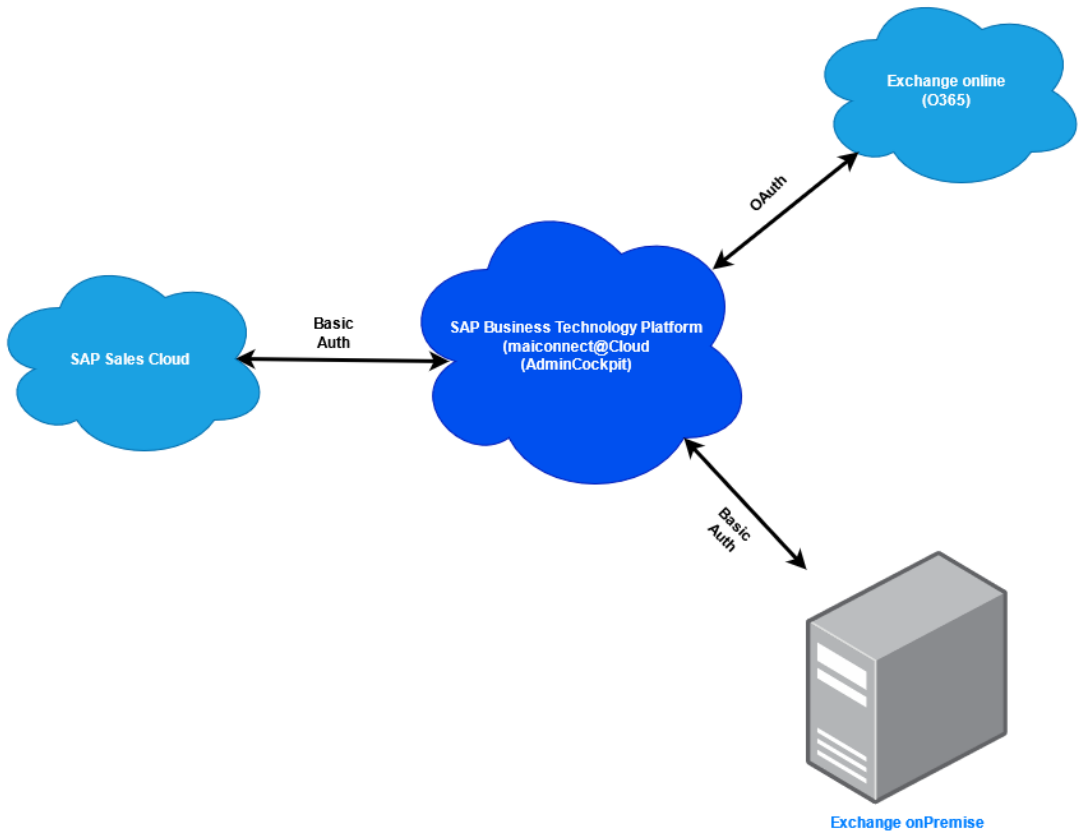
3.7 SYSTEM COPY 36

1 System landscape

maiConnect@Cloud is hosted on the SAP Business Technology Platform (BTP). Standard interfaces of SAP and Microsoft are used for the data exchange between SAP Sales Cloud and Microsoft Exchange (incl. Office365).

Communication between SAP Sales Cloud and SAP BTP is carried out by the Replication- and WebServices of the Sales Cloud. Upon creating/altering/deleting an object in the Sales Cloud a dedicated maiConnect@Cloud address is called.

The user communicates with the MS Exchange Server via Outlook Client as well and therefor gets all contacts, tasks and appointments. The direct communication with the MS Exchange Server renders the distribution of contacts, appointments and tasks to all Exchange-compatible devices (Blackberry, iPhone, ...) possible.



Picture 1: maiConnect system landscape (example)

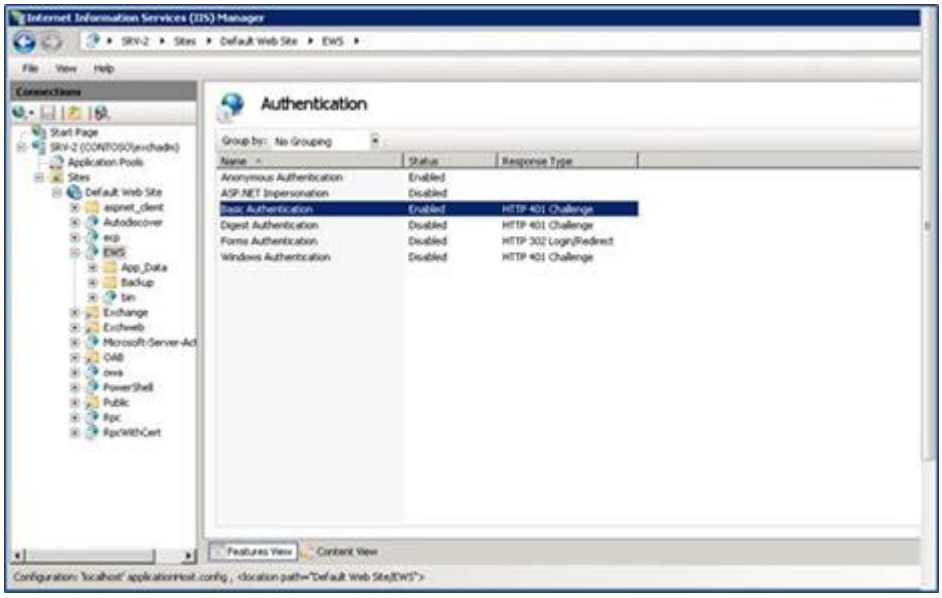
2 Exchange Setup

2.1 Activate EWS and Local Authentication

The administrator has to define the following custom settings for the Microsoft Exchange server

2.1.1 Local Exchange Server

The **Exchange Web Services (EWS)** have to be enabled, along with the **Anonymous Authentication** and **Basic Authentication.**



Picture 2: Screenshot for IIS configuration (example)

2.1.2 Office 365

In a cloud scenario OAuth must be activated on Exchange Online. By default, this is the case.

2.2 Setup mailbox access

To ensure access to the mailbox you can either use a **dedicated service user** or **OAuth** (only supported by Office365 for now).

Please note that access via a service user is only possible with Exchange onPrem. For Office 365, Microsoft only supports access via OAuth.

2.2.1 Dedicated Service User

maiConnect is using a dedicated Exchange user to update all groupware settings. Therefore this user has to have the necessary access authorization for the mailboxes of all other users.

Access rights can be assigned in various ways, which differ immensely in regards of the effort and subsequently required support. The methods listed here are examples and can be tailored, extended and combined to best meet the respective needs. Depending on the Exchange version and the system

environment not all of those methods might be available in every case. The following three sub-chapters describe different possibilities of granting access to the service user.

2.2.1.1 Rights on mailbox-database-level

A central Exchange user with the eligibility to read & write on all Outlook mailboxes is required. This eligibility can be granted using the following command:

```
Get-MailboxDatabase -identity “MailboxDatabase01” | Add-ADPermission -user "EXCH_ADMIN" -AccessRights GenericAll
```

This command only grants access to the Object MailboxDatabase01 - not to all Active Directory Objects. If there is more than one mailbox database this command needs to be executed for each database separately. However this command only grants access to all existing mailboxes; in case another mailbox will be added at a later point it needs to be re-executed (e.g. in terms of a scheduled script).

2.2.1.2 Allocation of rights via RBAC role

Provided that the RBAC roles are installed two commands have to be executed in the Exchange Management Shell (customized to the environment):

```
New-ManagementScope -Name "MAICONNECT_SCOPE" -RecipientRoot "contoso.de/Employee" -RecipientRestrictionFilter {RecipientType -eq "UserMailbox"}
```

At this point a limitation will be put on part of the users of the Exchange system. Based on that and by using the following command the access rights can be allocated:

```
New-ManagementRoleAssignment -Name " MAICONNECT_ROLE" -Role "ApplicationImpersonation" –User:”MAICONNECT_USER” –CustomRecipientWriteScope:”MAICONNECT_SCOPE”
```

The allocation of the ApplicationImpersonation role can be carried out without CustomRecipientWriteScope and will then refer to all users. Alternatively the CustomRecipientWriteScope can be adjusted to meet the respective needs (e.g. restricted to a group of users) to limit the access rights of the service user.

2.2.1.3 Individual Access to Mailboxes

If the Exchange admin user's access to the mailboxes shall be managed individually for each mailbox he needs the access rights to the respective folders (Calendar, Tasks, Contacts).

This can be arranged via script or directly from the mailboxes of the users. Both options are explained in the following:

Script

Using this script access to the calendar for all users can be established::

```
$rooms = Get-Mailbox -RecipientTypeDetails UserMailbox
$rooms | %{Add-MailboxFolderPermission $_":\Calendar" -User folderrights -
AccessRights Owner}
$rooms | %{Add-MailboxFolderPermission $_":\Tasks" -User folderrights -
AccessRights Owner}
$rooms | %{Add-MailboxFolderPermission $_":\Contacts" -User folderrights -
AccessRights Owner}
```

For just one mailbox:

```
Add-MailboxFolderPermission -Identity max.mustermann@maiconnect.com:\calendar -
<User>-AccessRights Owner
```

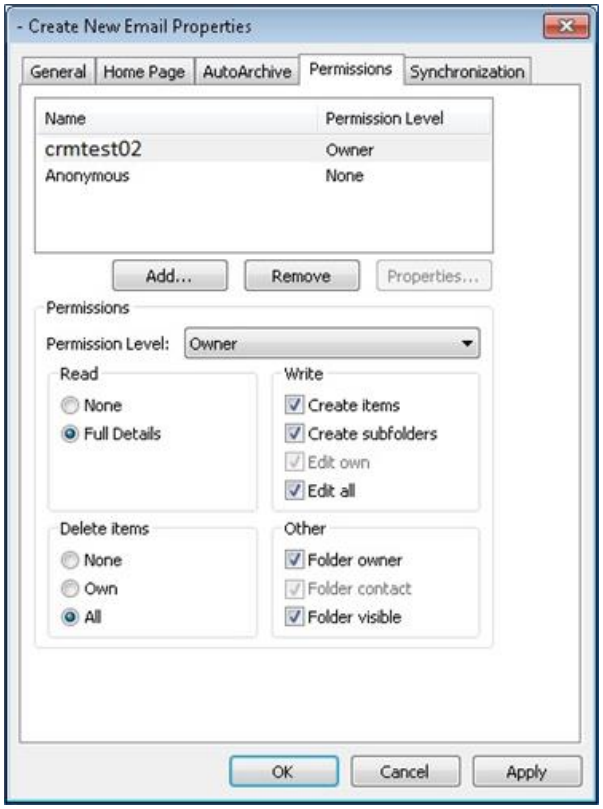
Full access:

```
Add-MailboxPermission -Identity max.mustermann@maiconnect.com -User
Maiconnect_User -AccessRights FullAccess -InheritanceType All
```

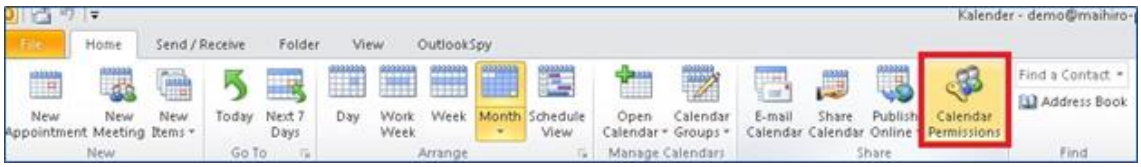
Directly from the mailbox

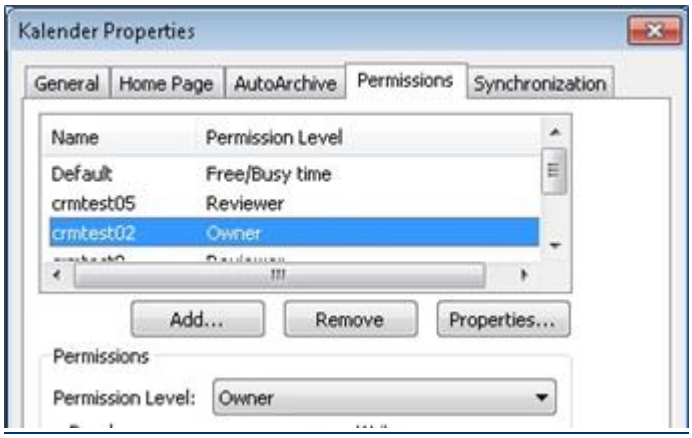
This approach is described in the following screenshots. In this example crmtest02 is used as a service user.

Tasks:

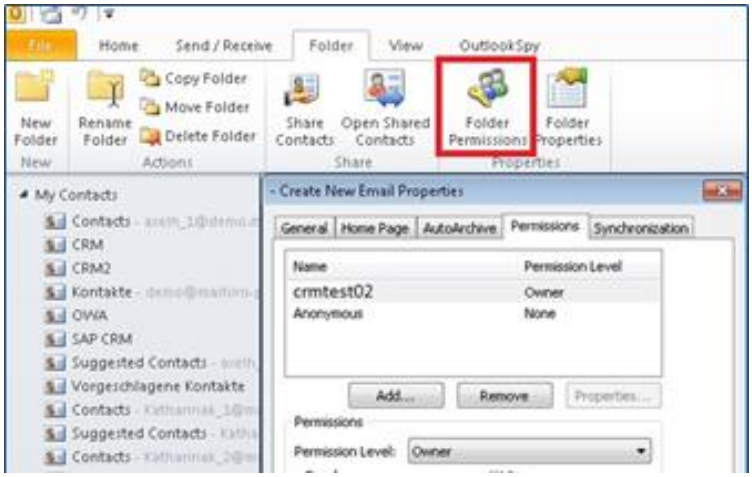


Appointments:



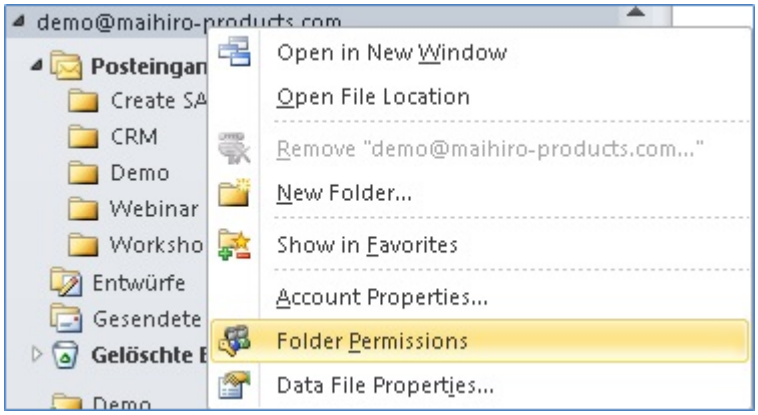


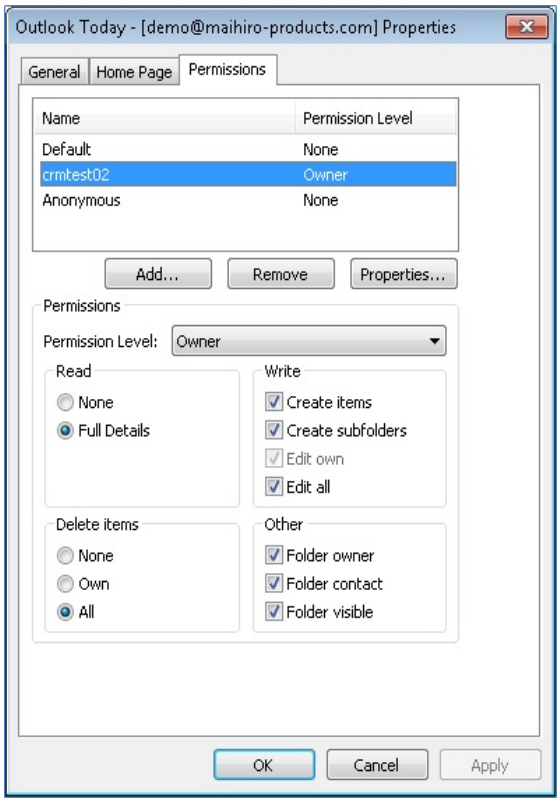
Contacts:



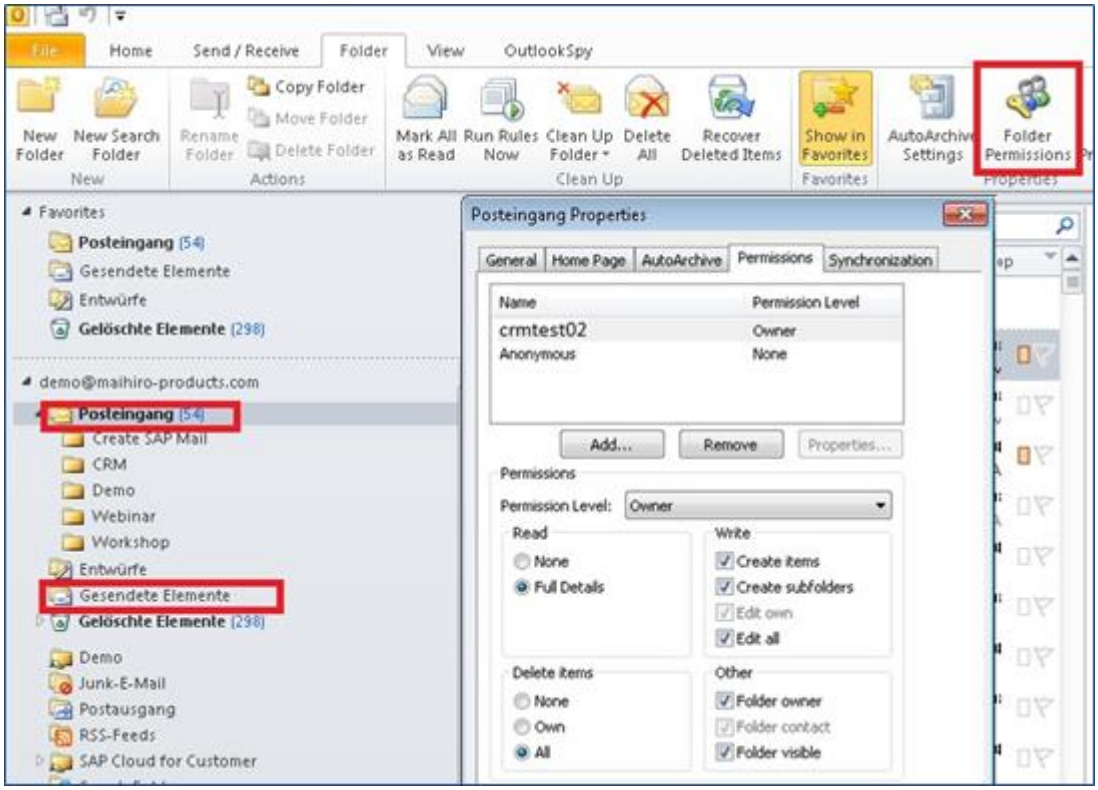
Mailbox:

If you use the e-mail and/or opportunity functionality the respective permissions have to be set for the whole mailbox.



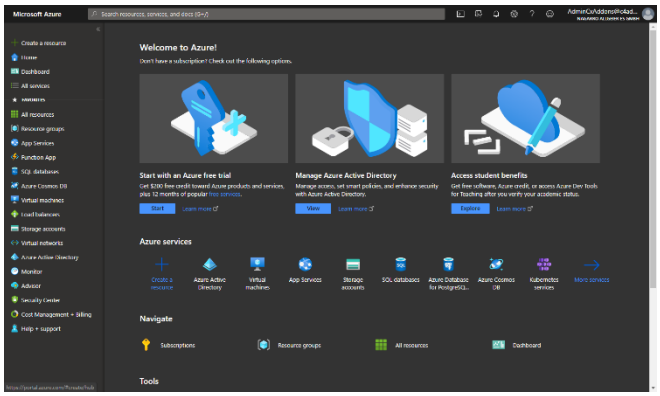


In order to transport E-Mails from the inbox and the „sent Items“ folder into the CRM the respective permissions have to be set for both folders.



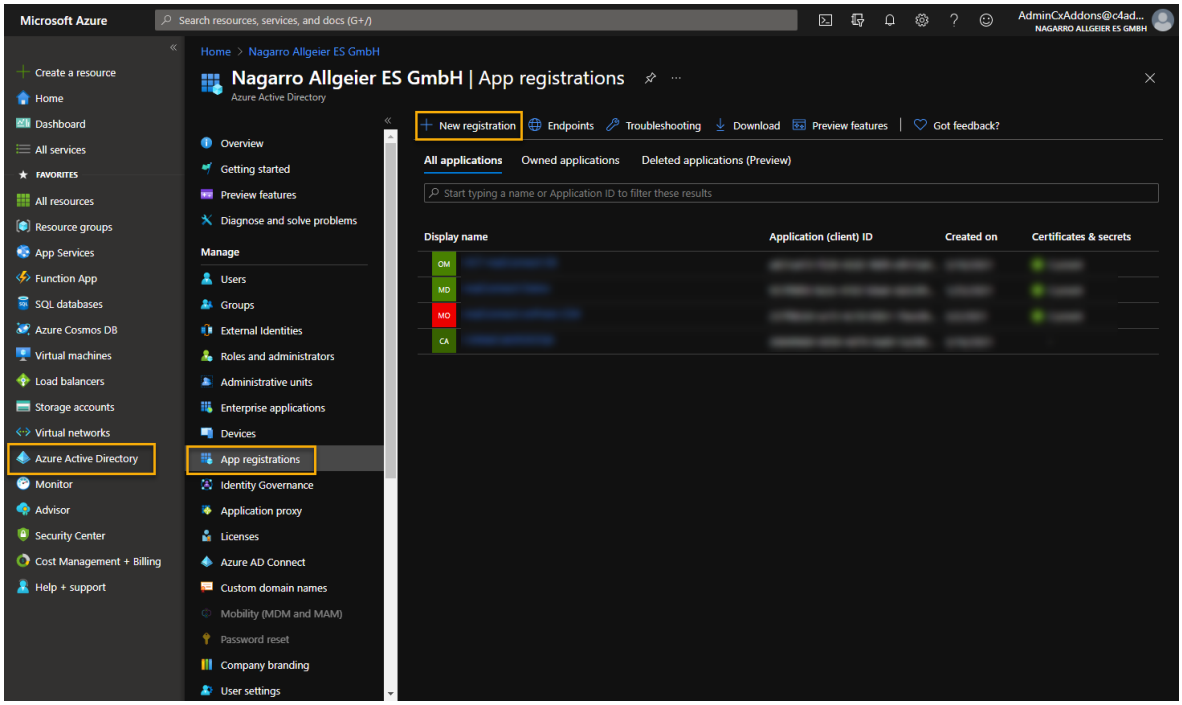
2.2.2 Authorization via OAuth (Office 365)

If Office365 is used the authorisation can be handled via OAuth. Therefore maiConnect@Cloud needs to be registered in the respective Azure AD - through the classic Azure Portal https://portal.azure.com/.

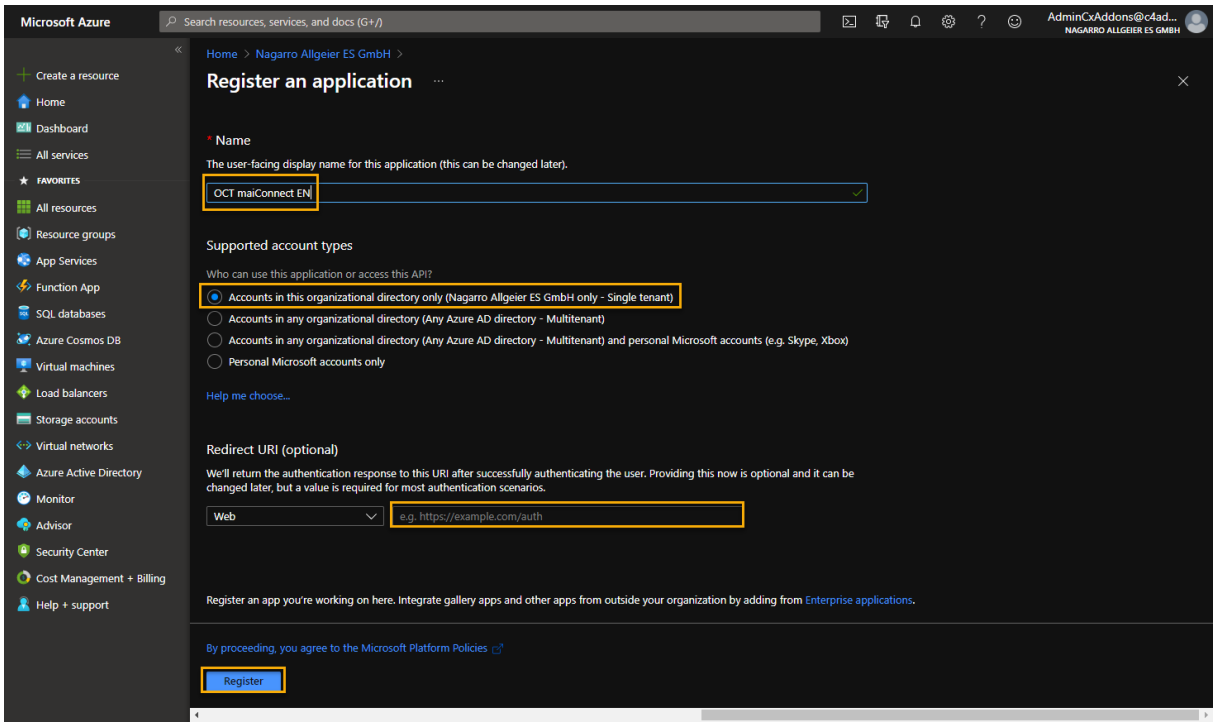


Log in with a user who has administrator rights.

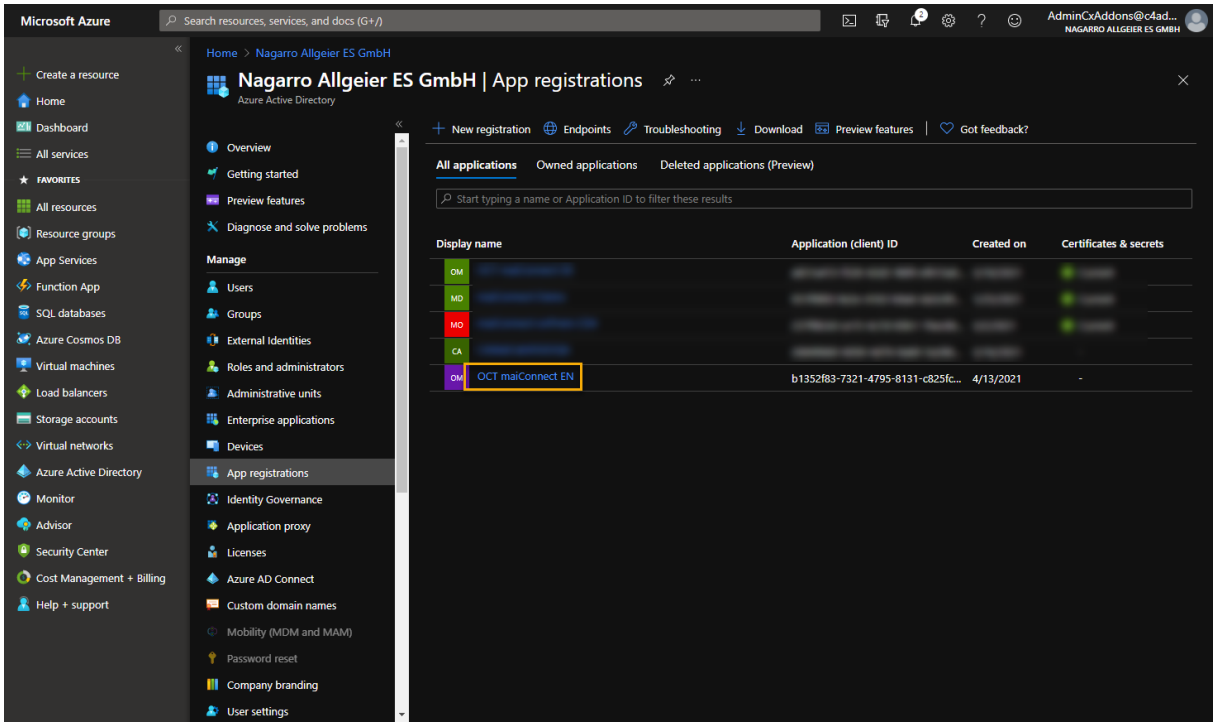
Navigate to "Azure Active Directory" -> "App registrations". Click “+ New registration".



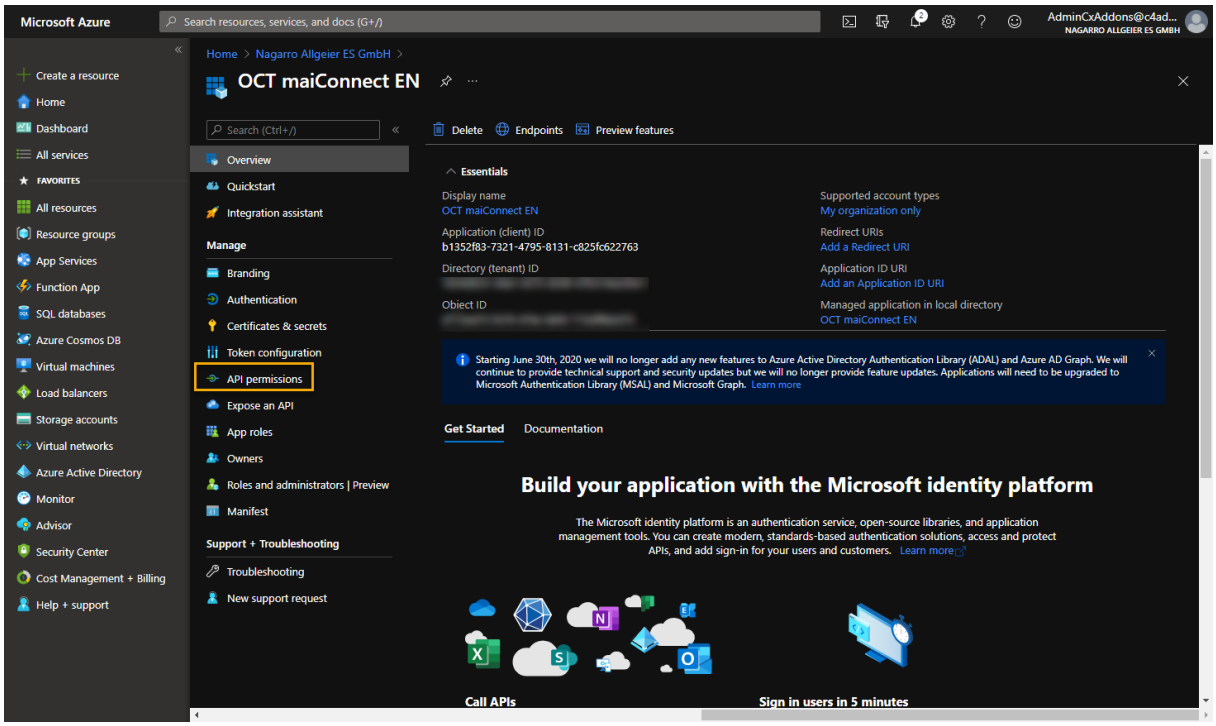
Provide a name for your application (e.g. “maiConnect”), select the account type as outlined in the screenshot below and leave the redirect URL empty. Click “Register”.



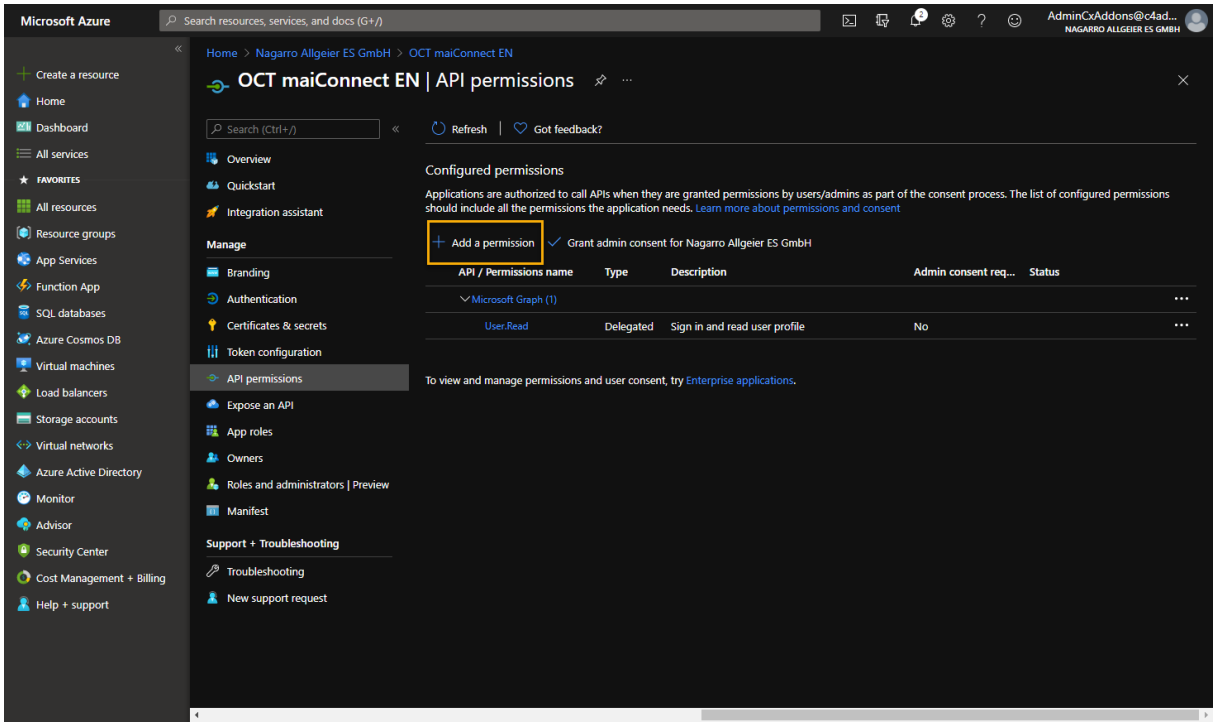
After this, maiConnect was successfully registered in your Azure AD.
Open your newly registered app by clicking the name



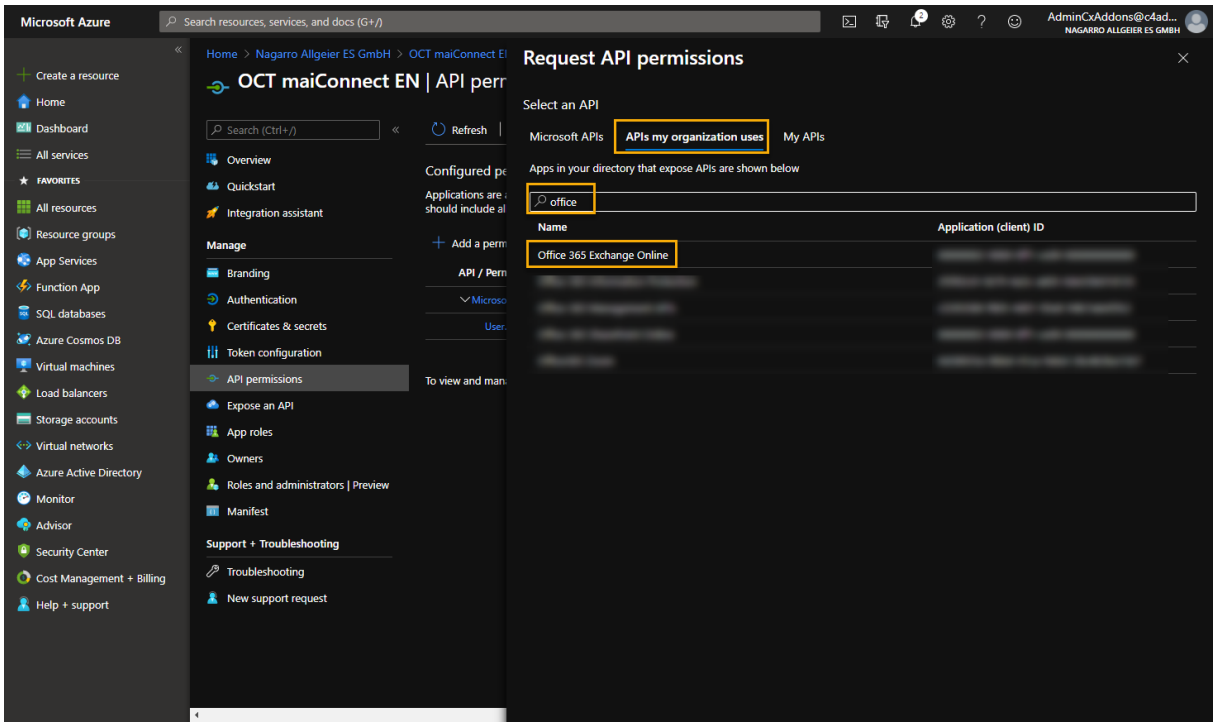
Head over to “App permissions”:



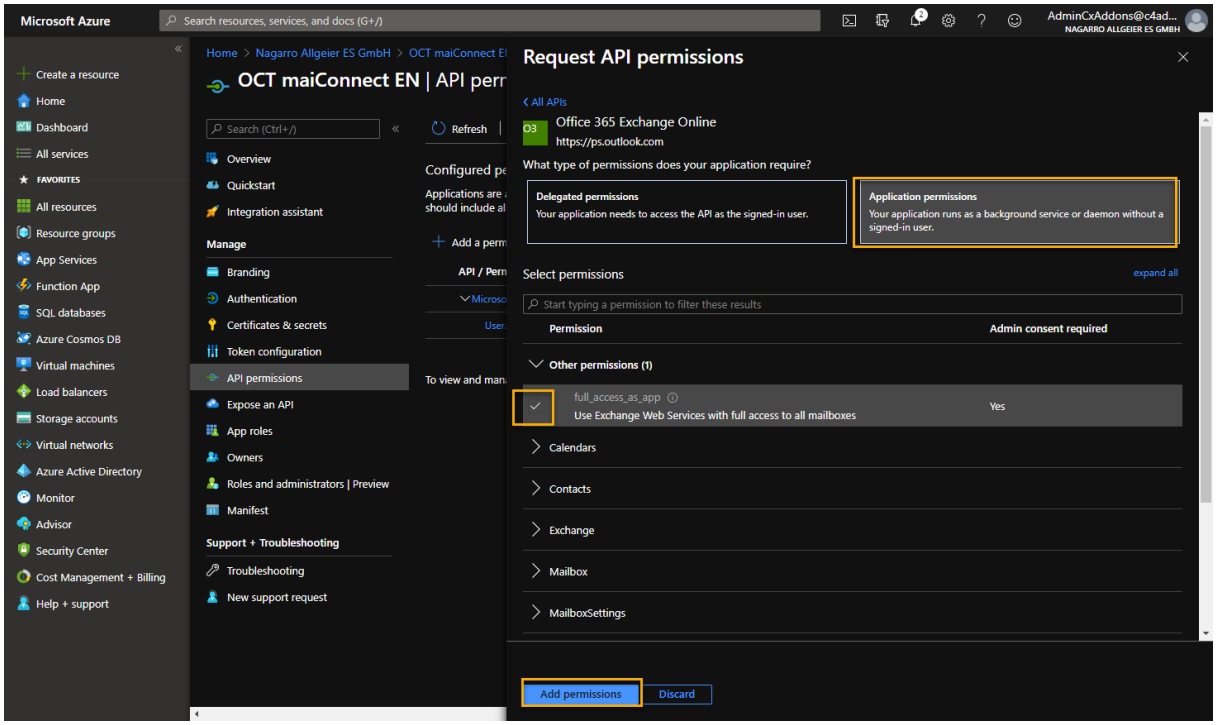
Add new permissions:



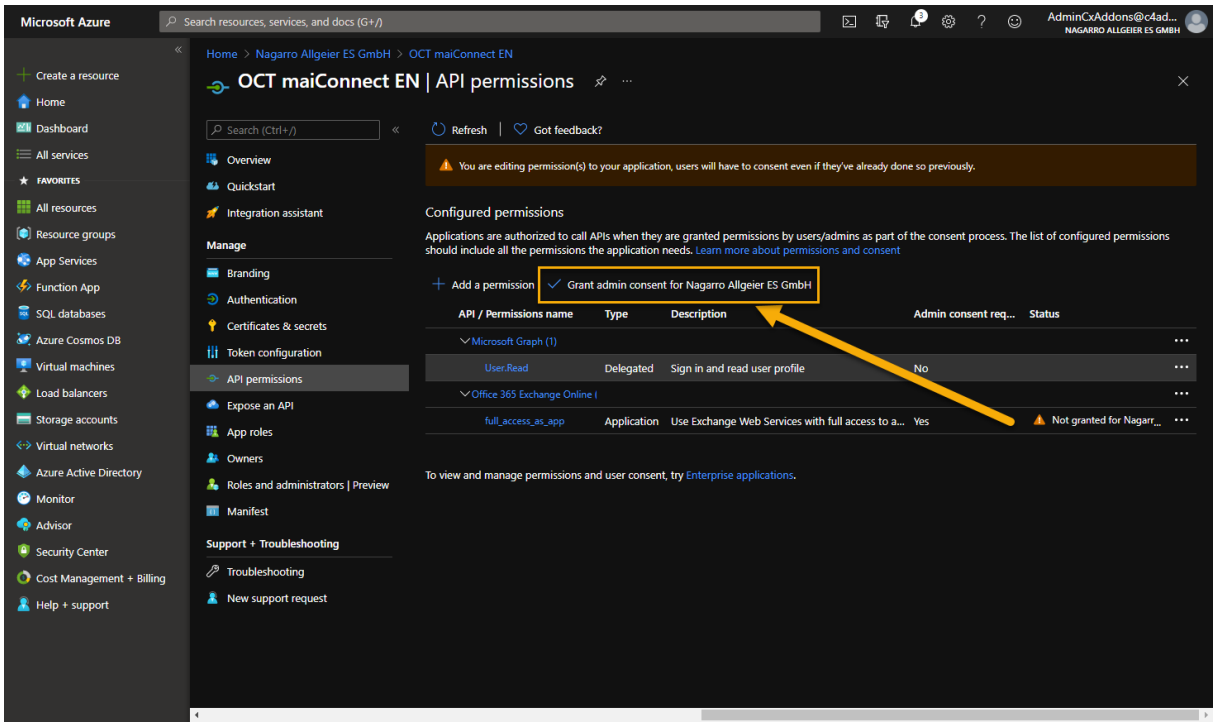
Select “APIs my organization uses”, search for “office” and select “Office 365 Exchange Online”:

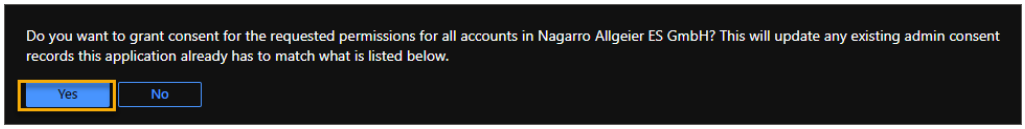


Choose “Application permissions” and select “full_access_as_app”. Add them by clicking the button below:

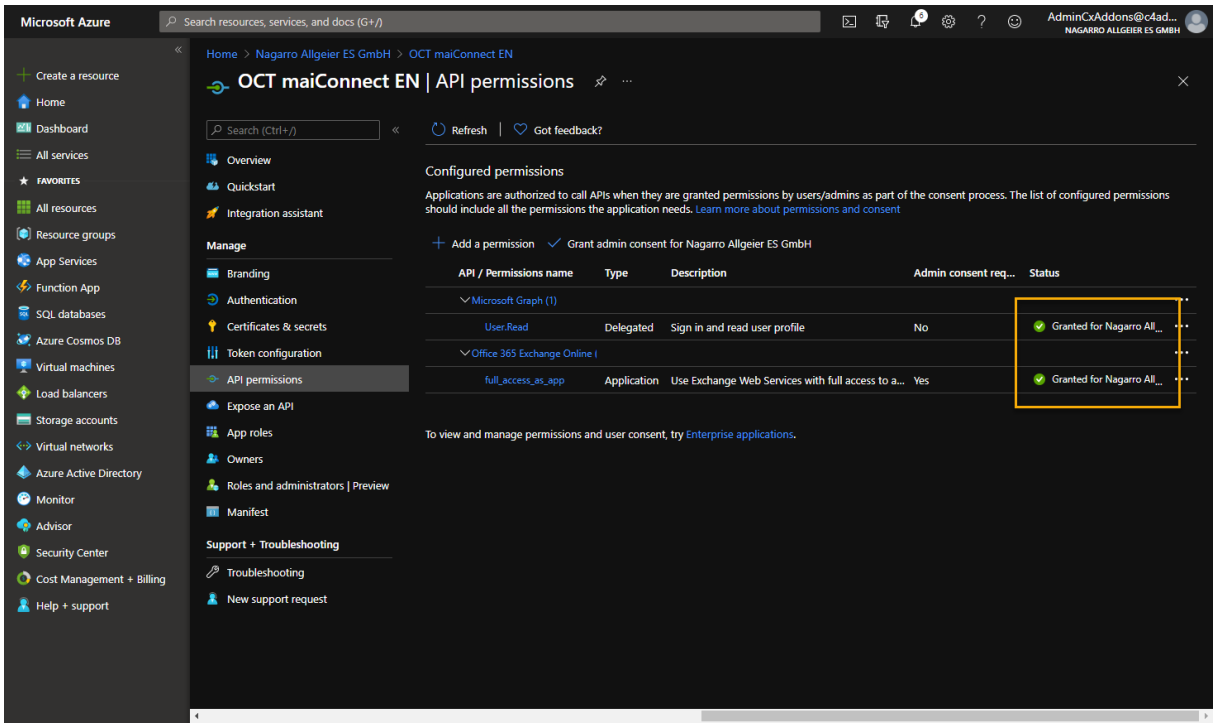


Now you have to grant admin consent for your organization:



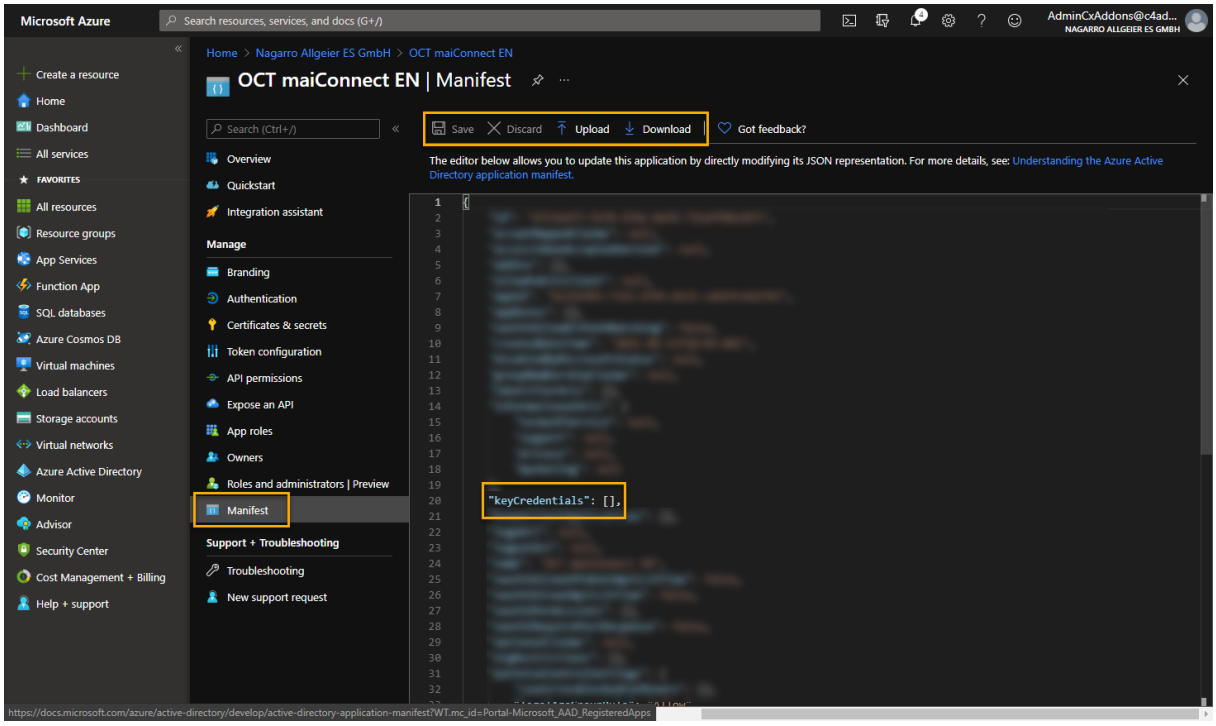


It should look like this now:



Now go to “Manifest” and exchange the following part:

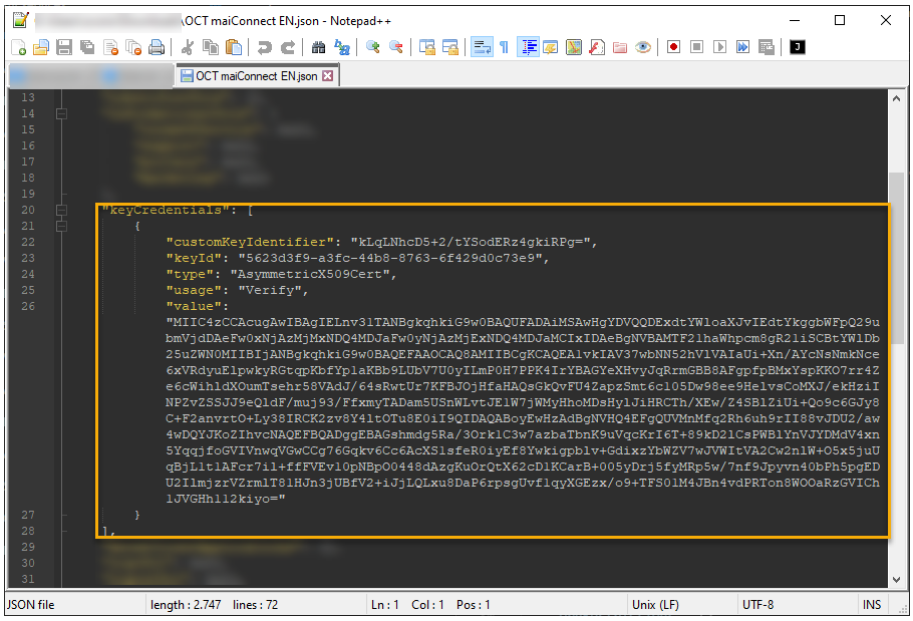
“keyCredentials”: [ ],



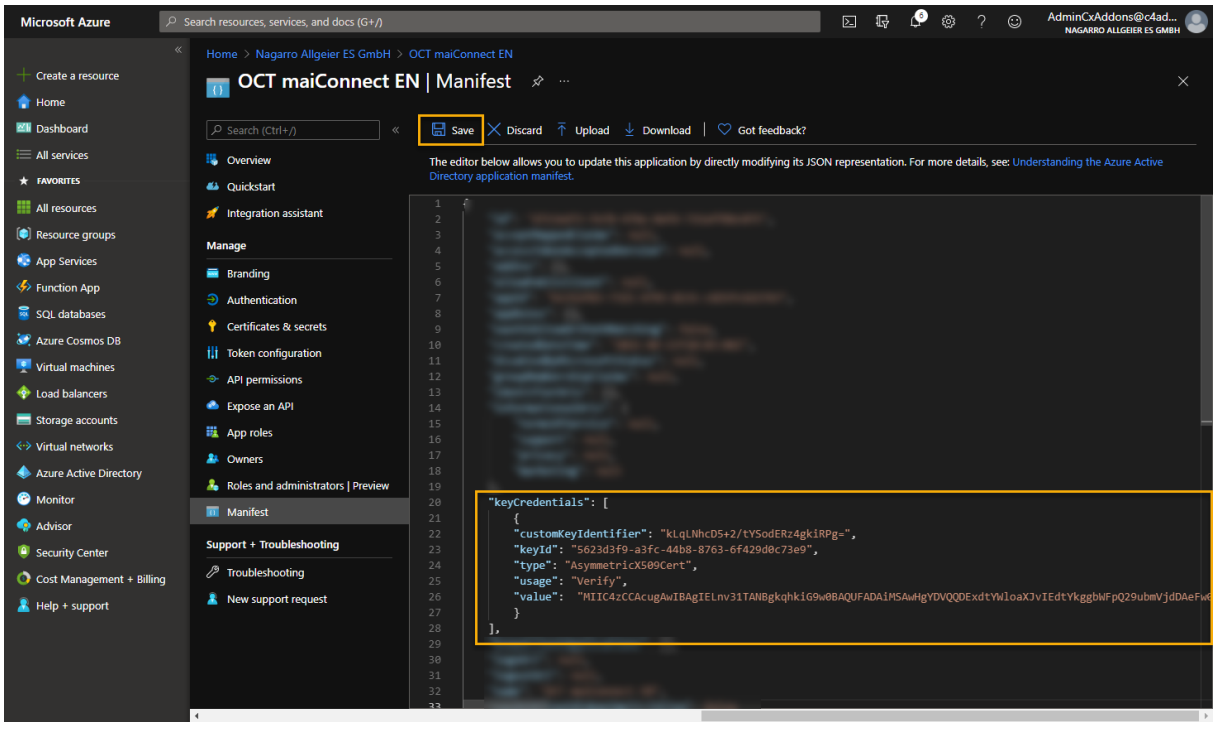
With the following part:


```
"keyCredentials": [
    {
      "customKeyIdentifier": "kLqLNhcD5+2/tYSodERz4gkiRPg=",
      "keyId": "5623d3f9-a3fc-44b8-8763-6f429d0c73e9",
      "type": "AsymmetricX509Cert",
      "usage": "Verify",
      "value":
"MIIC4zCCAcugAwIBAgIELnv31TANBgkqhkiG9w0BAQUFADAiMSAwHgYDVQQDExdtYWloaXJvIE
dtYkggbWFpQ29ubmVjdDAeFw0xNjAzMjMxNDQ4MDJaFw0yNjAzMjExNDQ4MDJaMCIxIDAeBgNVB
AMTF21haWhpcm8gR21iSCBtYWlDb25uZWN0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA1vkIAV37wbNN52hVlVAIaUi+Xn/AYcNsNmkNce6xVRdyuElpwkyRGtqpKbfYp1aKBb9LUbV
7U0yILmP0H7PPK4IrYBAGYeXHvyJqRrmGBB8AFgpfpBMxYspKKO7rr4Ze6cWihldXOumTsehr58
VAdJ/64sRwtUr7KFBJOjHfaHAQsGkQvFU4ZapzSmt6c105Dw98ee9HelvsCoMXJ/ekHziINPZvZ
SSJJ9eQldF/muj93/FfxmyTADam5USnWLvtJE1W7jWMyHhoMDsHylJiHRCTh/XEw/Z4SBlZiUi+
Qo9c6GJy8C+F2anvrtO+Ly38IRCK2zv8Y4ltOTu8E0iI9QIDAQABoyEwHzAdBgNVHQ4EFgQUVMn
Mfq2Rh6uh9rII88vJDU2/aw4wDQYJKoZIhvcNAQEFBQADggEBAGshmdg5Ra/3Ork1C3w7azbaTb
nK9uVqcKrI6T+89kD2lCsPWBlYnVJYDMdV4xn5YqqjfoGVIVnwqVGwCCg76Gqkv6Cc6AcXS1sfe
R0iyEf8YwkigpblV+GdixzYbWZV7wJVWItVA2Cw2nlW+O5x5juUqBjL1t1AFcr7il+ffFVEv10p
NBpO0448dAzgKuOrQtX62cD1KCarB+005yDrj5fyMRp5w/7nf9Jpyvn40bPh5pgEDU2IlmjzrVZ
rmlT81HJn3jUBfV2+iJjLQLxu8DaP6rpsgUvf1qyXGEzx/o9+TFS01M4JBn4vdPRTon8WOOaRzG
VICh1JVGHh112kiyo="
    }
  ],
```

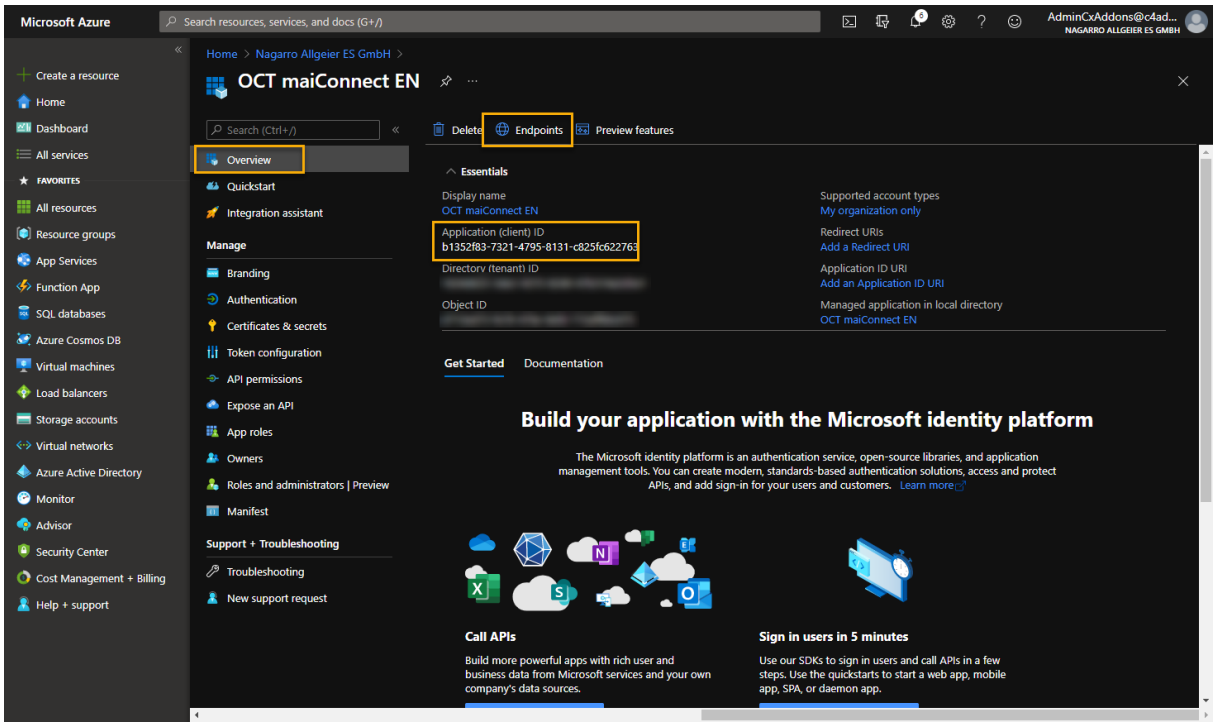

You can either directly edit the text right in the Azure Portal or you can download the manifest as JSON file, open it with an editor, exchange the relevant part, save it and re-upload the file as shown below.



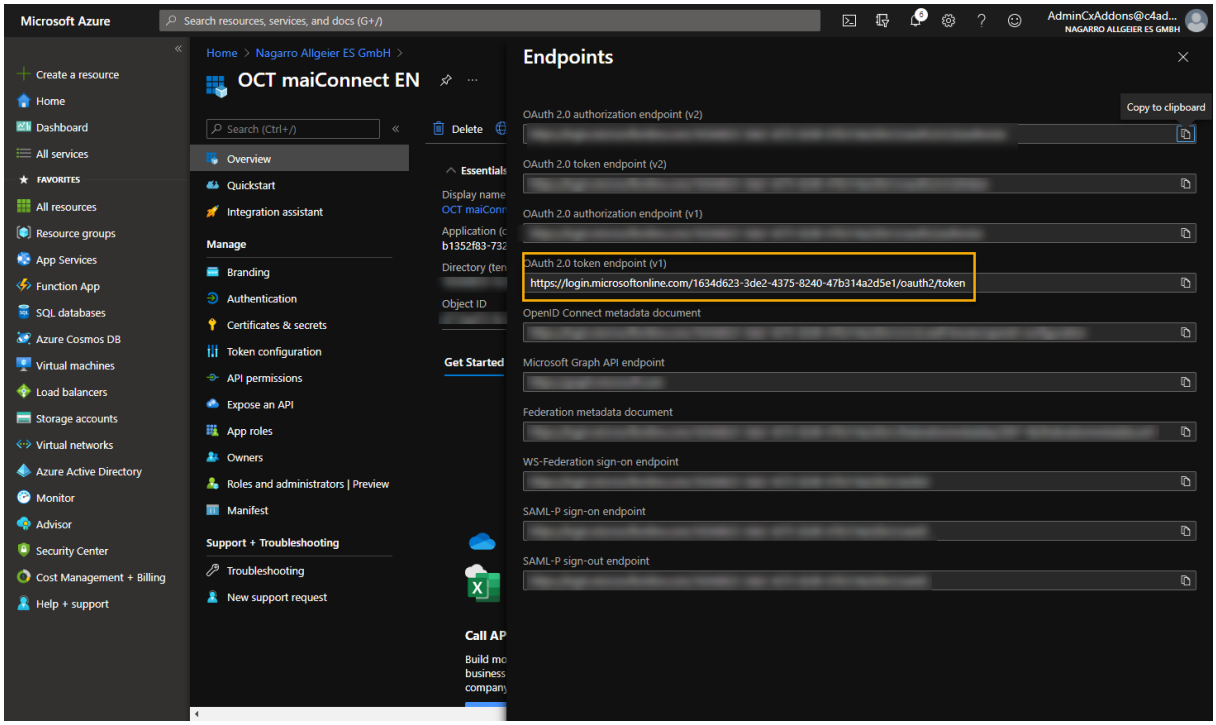
Make sure to SAVE the edited manifest:



Now go back to the overview of your app and note down the “Application (client) ID”. After this, click on “Endpoints”:



From the list of endpoints, select the one outlined in the picture below and provide this, along with the application ID to the business administrator responsible for maiConnect.



2.2.3 Note about the Azure API permissions

According to the above description in Microsoft Azure, maiConnect requires the application permission "full_access_as_app" for the EWS interface. This means, that the maiConnect application theoretically has access to all mailboxes.

The maiConnect AdminCockpit is used to define for which users the synchronization should take place. Only for the configured users an access to the mailbox takes place. Other mailboxes are not known to maiConnect at all. Therefore, it is hereby assured that no other mailboxes are accessed than the configured maiConnect users.

In addition, Microsoft Azure offers the possibility to control access to individual mailboxes via an ApplicationAccessPolicy. See the following page for more information:

https://docs.microsoft.com/en-us/powershell/module/exchange/new-applicationaccesspolicy?view=exchange-ps

To create a new ApplicationAccessPolicy the following command must be executed in Exchange Online PowerShell:

```
New-ApplicationAccessPolicy -AccessRight <ApplicationAccessPolicyRight> -
AppId <String[]> -PolicyScopeGroupId <RecipientIdParameter>
```

- AccessRight: DenyAccess / RestrictAccess.
- AppID: ID of the Azure AD application
- PolicyScopeGroupId: UPN of the user or name of the group

The simplest way to use policy is to create a RestrictAccess policy for an application with access to the necessary mailboxes. Access to mailboxes not stored in the policy is prevented.

2.3 Exchange throttling policy

The Throttling Policy can be used to limit the amount of connections per Exchange account. The parameter *EWSMaxConcurrency* is of special relevance. The following commands show how the Throttling Policy can be defined for maiConnect.

Please note: Office365 doesn't allow for this settings by default and some parameters do no longer exist for Exchange 2013.

Creating a policy name:

```
New-ThrottlingPolicy MaiConnect
```

Remove the Limitation of the Service Account:

```
Set-ThrottlingPolicy MaiConnect -RCAMaxConcurrency $null -RCAPercentTimeInAD $null - RCAPercentTimeInCAS $null -RCAPercentTimeInMailboxRPC $null - EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null - EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null - EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null
```

Exchange 2013

```
Set-ThrottlingPolicy MaiConnect -RCAMaxConcurrency Unlimited -EWSMaxConcurrency Unlimited -EWSMaxSubscriptions Unlimited -CPAMaxConcurrency Unlimited - EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited
```

Assign a service account to the policy:

```
Set-Mailbox "<maiConnectAdmin>" -ThrottlingPolicy MaiConnect
```

2.4 Connection between Exchange and SAP Business Technology Platform (BTP)

To access the Exchange server maiConnect is using Microsoft‘s standard EWS (Exchange Web Services). Requests for or changes to the Exchange server are executed by SAP Business Technology Platform (BTP) web services. Depending on the maiConnect customers network topology and security policies those web service calls can go through a proxy or firewall, which forward the requests to the respective Exchange server.

For the synchronisation from Exchange to BTP subscriptions are set up for every mailbox. Thus maiConnect is informed about changes (creation, update, deletion) to a subscribed mailbox by push notifications. The BTP is processing these notifications and sends an answer to the Exchange server. In case the BTP doesn’t respond (e.g. due to downtime) the Exchange server is sending the request again. If such a notification goes unanswered after multiple tries the subscription will be automatically deleted on the Exchange server. With the creation of a new maiConnect user subscriptions are automatically created. In case the subscriptions for certain mailboxes are deleted on the Exchange server there is a job in maiConnect which renews those subscriptions for the respective users. All changes missed in the meantime will be replicated with the help of a watermark.

During the creation of a subscription a call back URL is specified, to which the Exchange server notifications are to be sent to. This URL is also required for the setup of maiConnect on SAP Sales Cloud side and will be sent to the customer prior to the setup as it is customer specific.

Thus the customer has to ensure that the connection from BTP to Exchange via EWS is guaranteed. Likewise, the customer has to make sure that the subscription URL can be reached from the Exchange server. Additional information can be found here: https://msdn.microsoft.com/en-us/library/office/dn458791(v=exchg.150).aspx

Please note

The network environment is customer specific and therefore it’s up to them to care for the abovementioned steps. Please make sure that the communication between BTP and Exchange server is not blocked by a reverse proxy or a firewall.

The communication between BTP and Exchange is encrypted by using SSL certificates. The SAP BTP's certificate is signed by a root certificate authority (CA) called Baltimore Cybertrust. General the root certificate from that CA is already available in the Exchange.

In case of push notifications a connection is established from the exchange server to the BTP. If that connection can't be established it means that the ssl handshake might not be successfull. In this case it is good to check with the client if the root CA certificate from Baltimore Cybertrust is installed.

If the connection to the Exchange Server is secured by SSL with a certificate, the certificate must have been created by certain trusted certification authorities. A list of certification authorities accepted by SAP can be found here:

https://wiki.scn.sap.com/wiki/display/CLOUD/Trusted+Certificate+Authorities

In case proxy servers are installed at a customer and the connection from Exchange to BTP can't be established (Push notification not received by BTP), it might be necessary to establish a direct connection w/o using proxies.

Following article explains how this can be done:

https://msdn.microsoft.com/en-us/library/aa579128(v=exchg.80).aspx

3 SAP Sales Cloud Settings

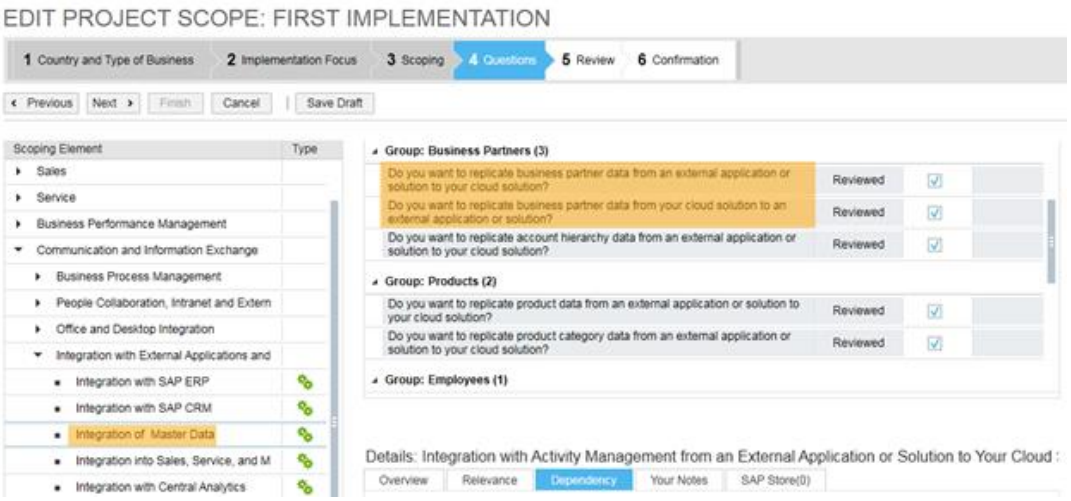
3.1 WebServices

SAP Sales Cloud is offering different WebServices which can be used by maiConnect to realise the synchronisation between Sales Cloud and Exchange. Therefore it has to be ensured that those WebServices can be accessed from the Sales Cloud tenant (activated by default).

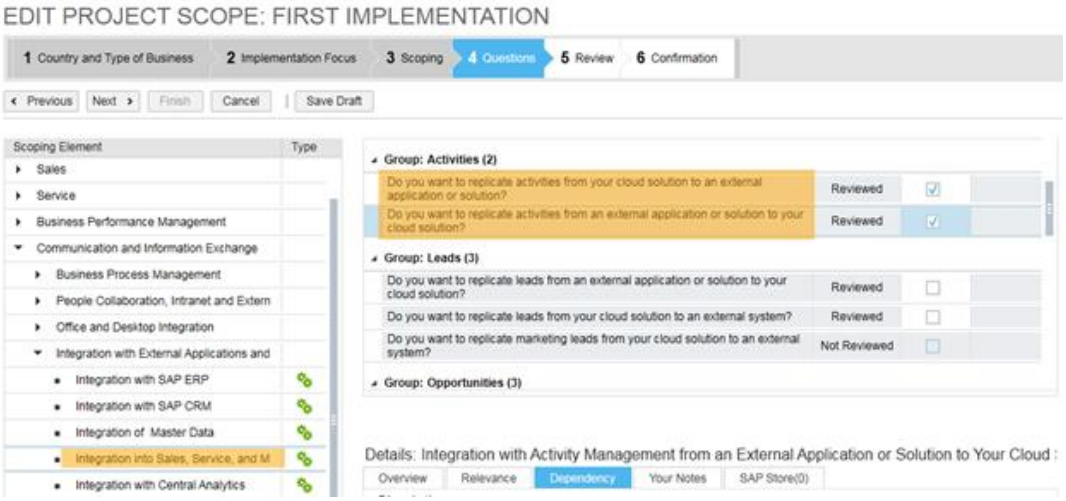
3.2 Business Configuration

In order to use the replication services of the Sales Cloud, your tenant's project scope (Business Configuration → All current Projects → Edit Project Scope) has to include the following points (depending on the maiConnect features you use):

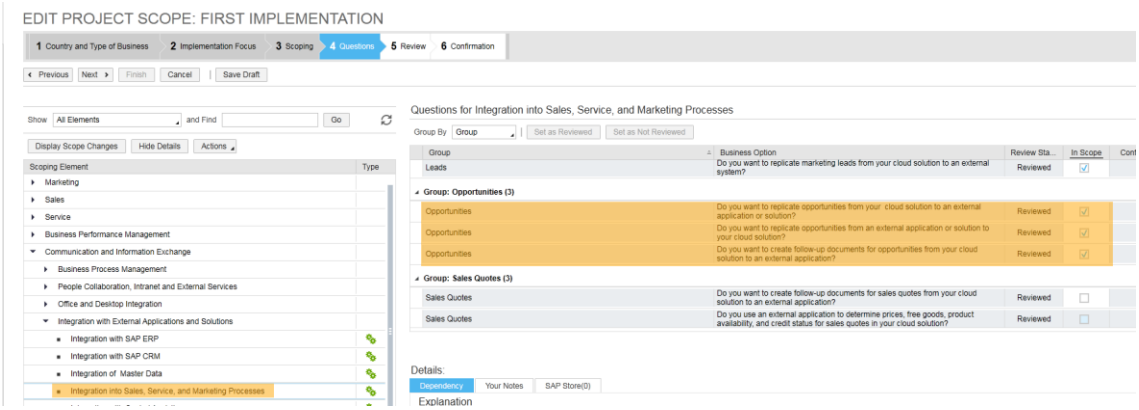
Exchange of contact persons



Exchange of appointments, tasks and eMails:



Exchange of opportunities (only enterprise licence):



3.3 Communication User

For communication between Sales Cloud and SAP Business Technology Platform a communication user with the following access rights needs to be set up with the following access rights.

> It can be useful to group this access rights in an own maiConnect role.

Work center ID	Work Center View ID	Work Center View Name	Reason
Business Area BuiltIn Services And Support	BC_BUILTINSERVICESANDSUPP	Business Area BuiltIn Services And Support	
Business Area Business Performance Management	BC_BUSINESSPERFORMMGMT	Business Area Business Performance Management	
Business Area Communication And Information Exchange	BC_COMMUNICANDINFEXCHANGE	Business Area Communication And Information Exchange	
Business Area Employee Self Service	BC_EMPLOYEESELFSERVICE	Business Area Employee Self Service	
Business Area General Business Data	BC_GENERALBUSINESSDATA	Business Area General Business Data	

Work center ID	Work Center View ID	Work Center View Name	Reason
Implementation Projects	BC_IMPLEMENTATIONPROJECTS	Implementation Projects	
Project Administration	BC_PROJECTADMINISTRATION	Project Administration	
Reports	BC_REPORTS	Reports	
Business Partners	BPM_BUSINESSPARTNERS	Business Partners	Synchronization of contact persons
Employees	BPM_EMPLOYEES	Employees	Synchronization of contact persons
Service Agents	BPM_SERVICEAGENTS	Service Agents	
Common Authorizations	CC_COMMON	Common Authorizations	Communication
Common Authorizations for Employees	CC_COMMONEMPLOYEESELFSERVICE	Common Authorizations for Employees	Communication
Common Authorizations for Users	CC_COMMONPERSONALWORK	Common Authorizations for Users	Communication
Communication Certificates	CERTIFICATE_ASSIGNMENT_WCVIEW	Communication Certificates	Communication
Account Hierarchy	CODACCHIERWCV	Account Hierarchy	Synchronization of contact persons
Visit Planner	CODACCOUNTVISITWCV	Visit Planner	Synchronization of activities
Accounts	CODACCOUNTWCV	Accounts	Synchronization of contact persons
Activity Lists	COD_ACTIVITY_LIST_WCVIEW	Activity Lists	Synchronization of activities

Work center ID	Work Center View ID	Work Center View Name	Reason
Appointments	COD_APPOINTMENT	Appointments	Synchronization of activities
Contacts	COD_CONTACT_WCV	Contacts	Synchronization of contact persons
E-Mails	COD_EMAIL	E-Mails	Synchronization of activities
Messaging	COD_MESSAGING_WCVIEW	Messaging	Synchronization of activities
Phone Calls	COD_PHONECALL	Phone Calls	Synchronization of activities
Individual Customers	COD_SEOD_ACCOUNTWL_WCVIEW	Individual Customers	Synchronization of contact persons
Target Groups	COD_TARGETGROUP	Target Groups	Synchronization of contact persons
Verkauf	COD_MKT_PROSPECTWC	Leads	Synchronization of leads
Verkauf	COD_QUOTE_WCVIEW	Quotes	Synchronzation of quotes
Tasks	COD_TASK	Tasks	Synchronization of activities
Tours	COD_VISIT_TOUR_WCVIEW	Tours	Synchronization of activities
Visits	COD_VISIT_WCVIEW	Visits	Synchronization of activities
Communication Systems	COMMUNICATION_SYSTEM_WC_VIEW	Communication Systems	Communication
Delegates	EMPSUBS	Delegates	
Sales Intelligence	EXTERNALBUSINESSPARTNERWCVIEW	Sales Intelligence	

Work center ID	Work Center View ID	Work Center View Name	Reason
iPad Offline	IPAD OFFLINE	iPad Offline	Download of code lists
Background Jobs	ITS_BACKGROUNDJOBS	Background Jobs	
Flexibility Change Log	ITS_KEYUSERCHANGELOG	Flexibility Change Log	
Service Explorer	ITS_SERVICE_EXPLORER	Service Explorer	
Communication Arrangements	MESSAGE_BASED_COMMUNICATION_AR	Communication Arrangements	Communication
Notification of Delegates	NOTIFICATIONSUBS	Notification of Delegates	
OData Service Explorer	ODATA_SERVICE_EXPLORER_WCVIEW	OData Service Explorer	Access to SAP Sales Cloud with OData
ID Mapping for Integration	OIM_WCVIEW	ID Mapping for Integration	
Business Partner Changes	PARTNER_CHANGE_HISTORY_WCV	Business Partner Changes	Synchronization of contact persons
Routes	ROUTE_WCVIEW	Routes	Synchronization of activities
General Settings	SEOD_ADMIN_SETUP_WCVIEW	General Settings	Communication

Business User vs. Technical User

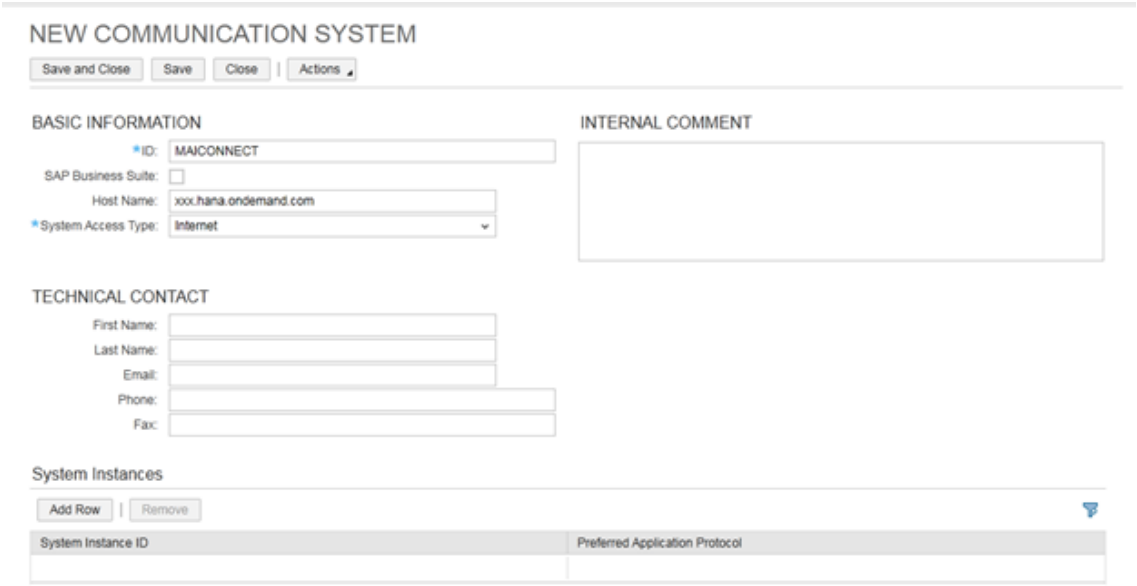
Normally a technical user should be used to communicate between two systems through a communication arrangement. As it is not possible at the moment to synchronize attachment objects with this technical user a business user as communication user is mandatory.

3.4 Setup communication scenarios

The maiConnect Callback address needs to be registered for a communication scenario in the corresponding communication arrangements. A communication arrangement is established for a communication system.

3.4.1 Communication System

Open the Administrator view and select "Application and User Management->Communication Systems". Select „New“.



Basic Information:

Parameter	Value
ID	unique name, e.g. „maiconnect“
SAP Business Suite	mark with "x"
Host Name	callback address (provided by maiConnect support) **without “https://”**
System Access Type	Internet

System Instances: Here it is important to select “5 – WebService” as the “Preferred Application protocol”.

Finally the communication system needs to be activated (Actions -> Set to Active) and saved.

3.4.2 Communication Arrangements

Switch to "Application and User Management->Communication Arrangements“.

The following communication arrangements need to be created for the different communication scenarios:

- Business ActivityReplication to SAP Business Suite

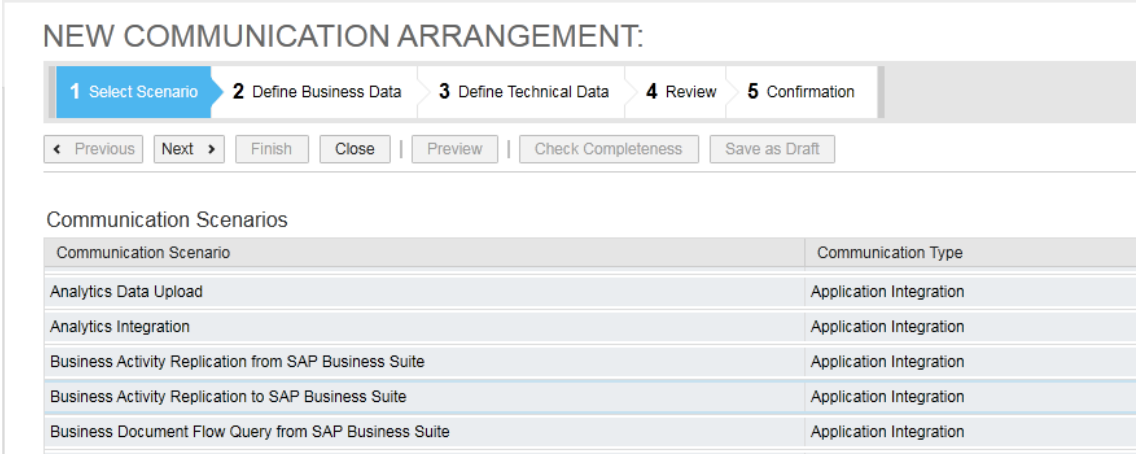
- Business Partner Replication to SAP Business Suite

In case your maiConnect license includes opportunity synchronization, then the following communication arrangement must also be created:

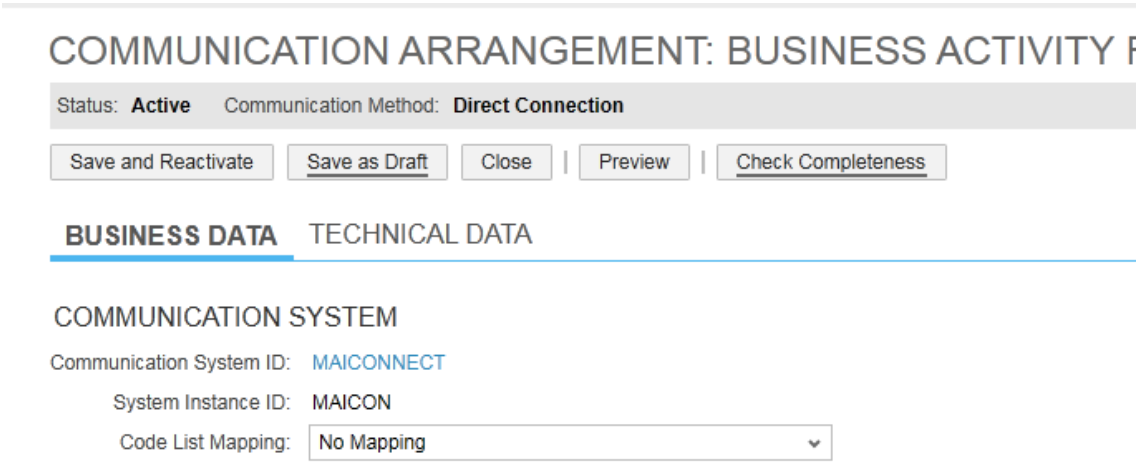
- Opportunity Replication to SAP Business Suite

The setup is the same for every scenario and is explained below for the “Business ActivityReplication to SAP Business Suite“.

Please select “New” in communication arrangements view and select the according scenario.

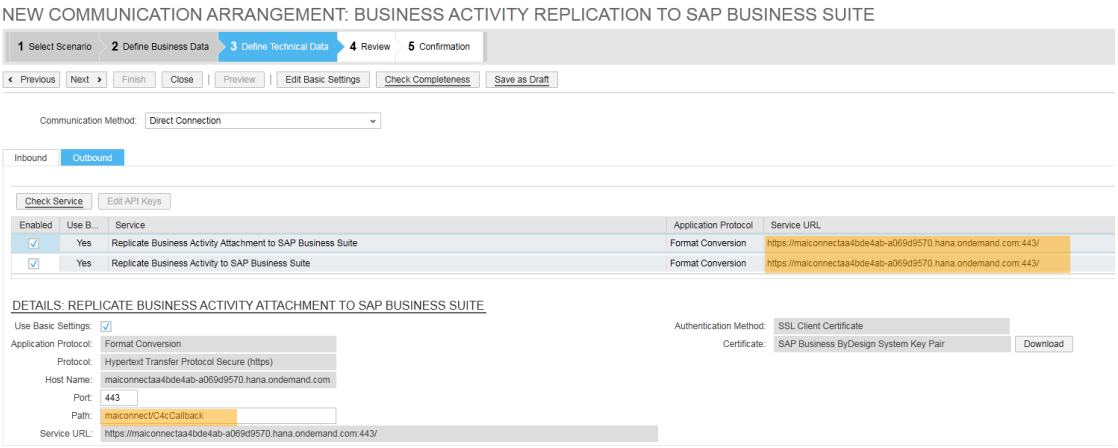


Click "Next". Connect the communication arrangement with the newly created communication system. Choose for "Code List Mapping" the value "No mapping".



Click "Next" and go to “Edit advanced settings”.

Select the tab “Outbound” and enter “maiconnect/C4cCallback?sap-client=<SAP_CLIENT_NUMBER_ENTERED_IN_COM_SYSTEM>” as path. Press enter to update the displayed fields. Do this for all listed services:



Click „Next“ and then „Finished”.

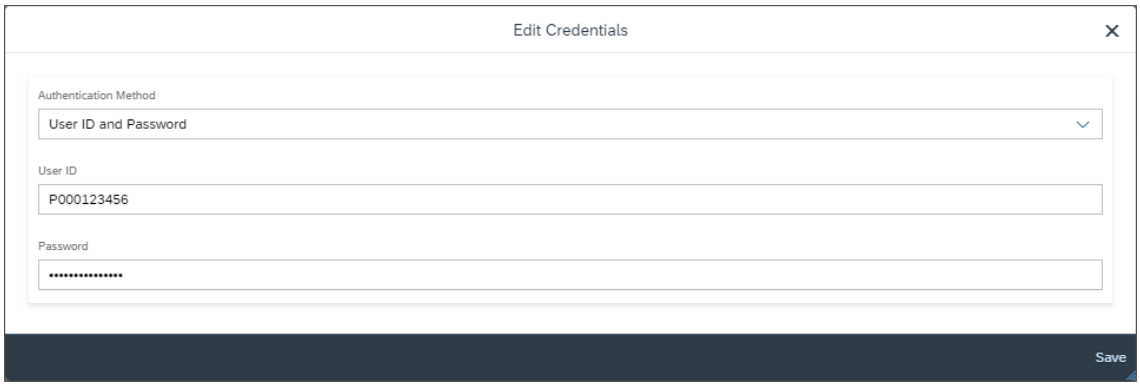
3.5 Event notifications

Instead of using the communication arrangements, synchronisation can also be handled via event notifications. To set this up, open the Administrator page in SAP C/4 Hana and choose "Event Notification" in the "General Settings" section. Add a new consumer:

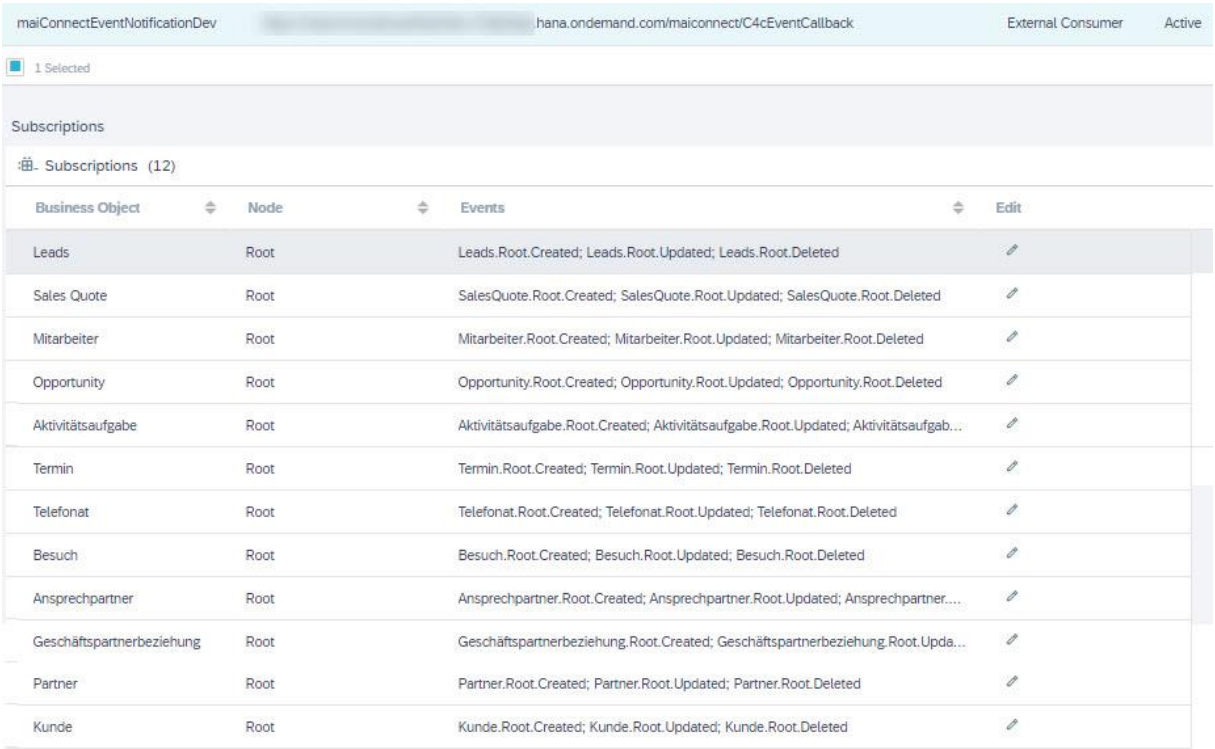
Parameter	Value
Type	External consumer
Name	maiConnectEventNotifications
Endpoint	callback address (provided by maiConnect support). The address must end with “hana.ondemand.com/maiconnect/C4cEventCallback”.

For the next step you need a SAP user. To do this, register at https://account.hana.ondemand.com/ - here you will receive a user ID (10 digits, starting with a P) and assign a password. If you already have a P- or S-user from SAP, you can of course skip this step.

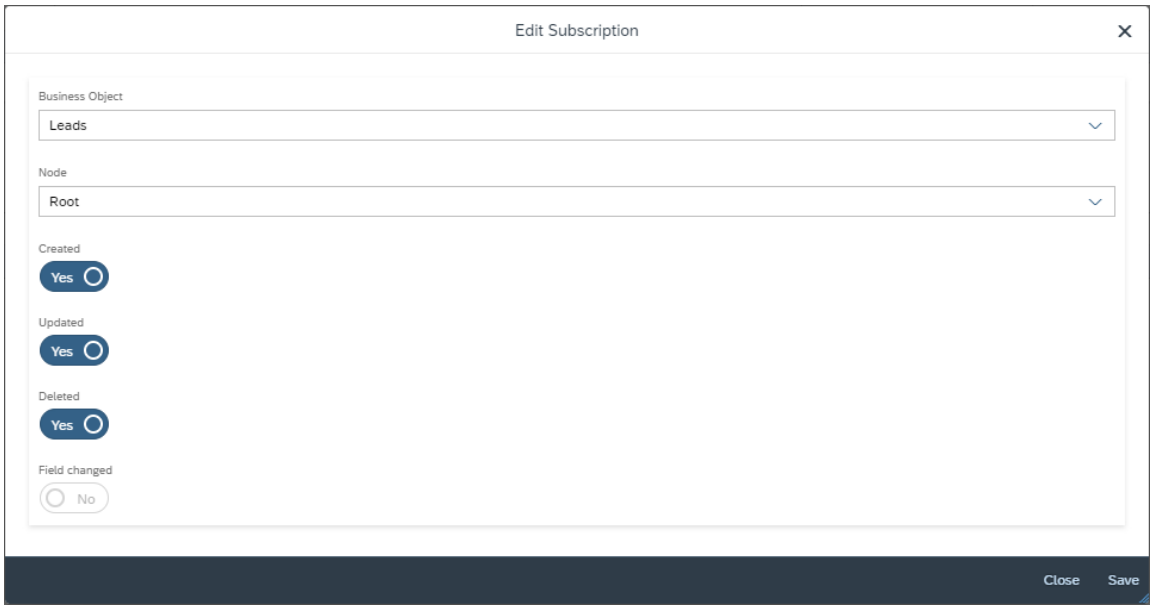
Now go back into the Sales Cloud event notification settings, select the previously created consumer and click on “Edit credentials”. Select “User ID and Password” as authentication method and enter the credentials of your P- or S-user. Click on save to save the changes.



Afterwards add subscriptions for those objects you want to exchange with maiConnect by clicking on “Add”.



Please always select the options for creation, updates and deletion. For Leads it would look like this:



Afterwards save the settings.

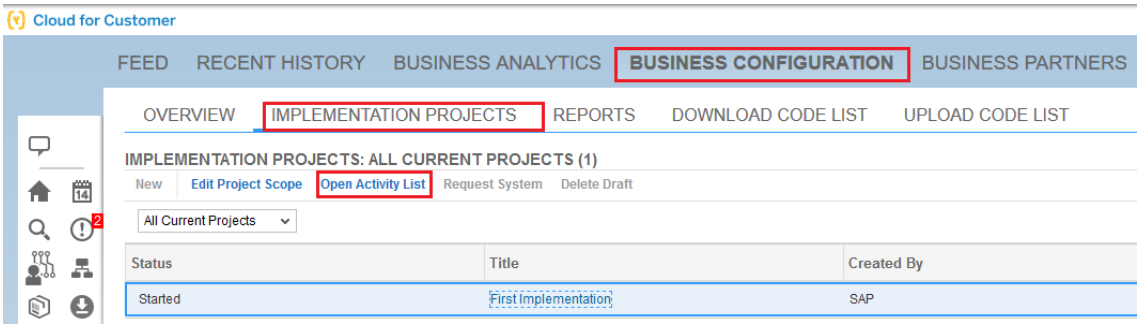
Please note:

To complete this step, the maiConnect support requires the user ID of the SAP user you are using (only the ID, not the password). Please provide the ID via your maiConnect deployment consultant or via support (support.cxaddons@nagarro.com).

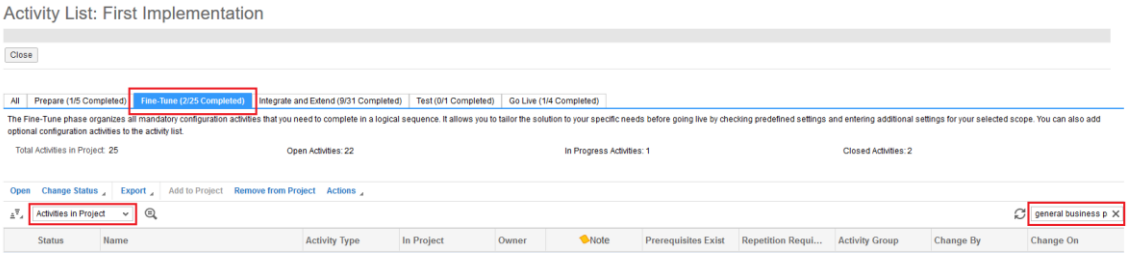
3.6 Create relationtype

Business partners of type "person" can be synchronized by maiConnect. This is done via a unique relationship that can be maintained on the contact, account or account team.

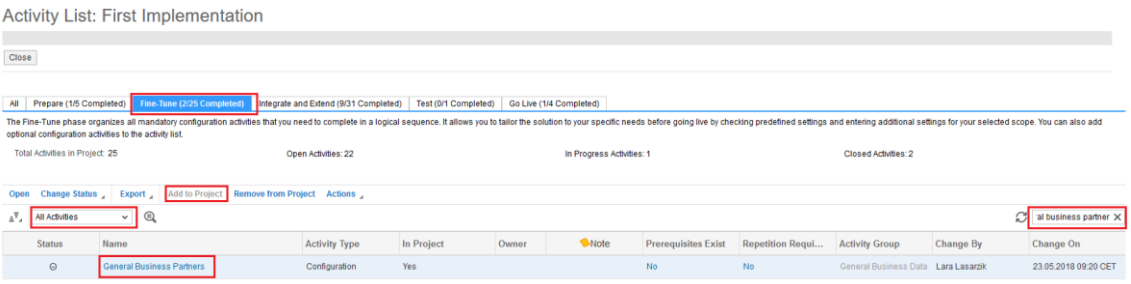
To create the relationship, open the "Business Configuration" in the SAP Sales Cloud, open the "Implementation Projects" sub-work center and navigate to the activity list:



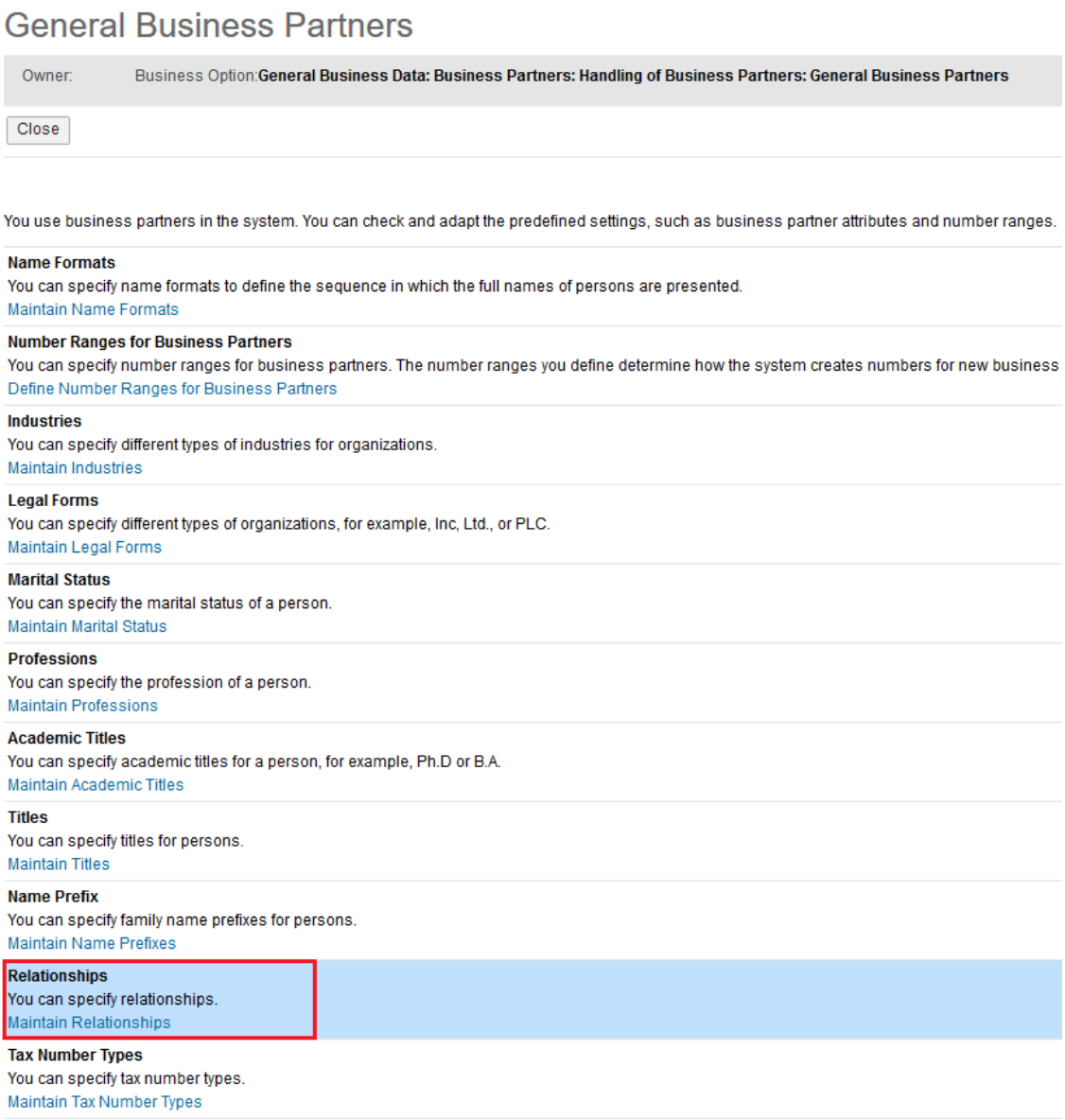
Open the "Fine-Tuning" tab and check whether the task "General Business Partner" is already included in your project.



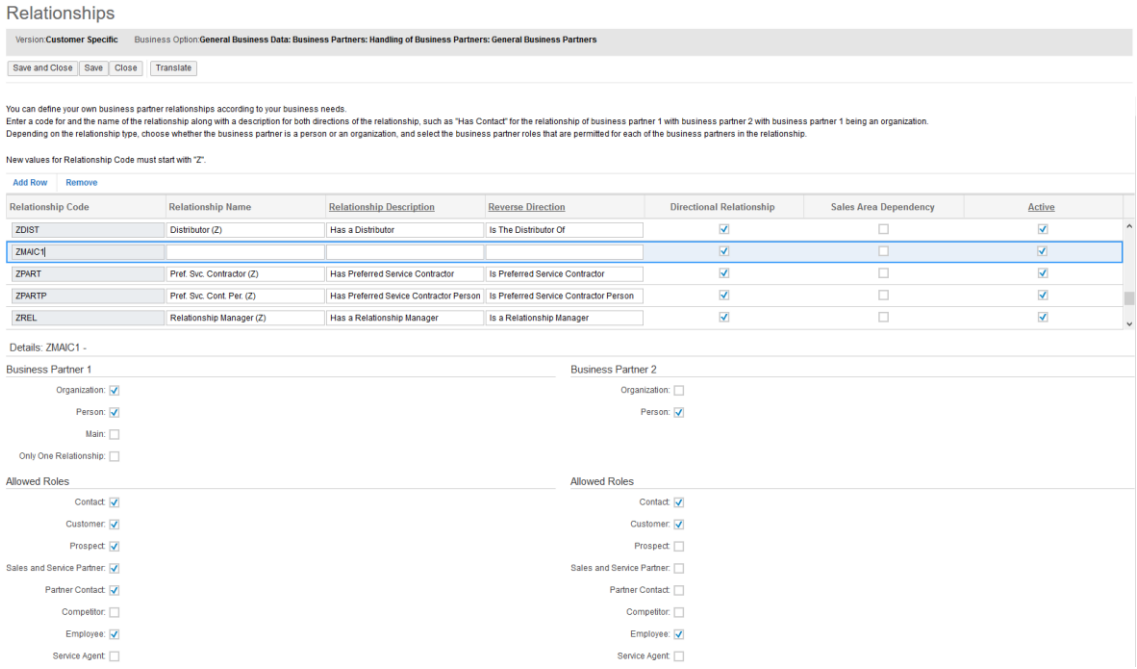
If this task is not included in your project, change the view to "All Activities", search for the task "General business partner" and add it to the project:



Open the task "General Business Partner". Under "Relationships" you can maintain the relationships for the Sales Cloud system:



Please create a new relationship as shown in the following screenshot. As relationship code "ZMAIC1" should be used.


Relationships
Version:Customer Specific
Business Option:General Business Data: Business Partners: Handling of Business Partners: General Business Partners
Save and Close
Save
Close
Translate
You can define your own business partner relationships according to your business needs.
Enter a code for and the name of the relationship along with a description for both directions of the relationship, such as "Has Contact" for the relationship of business partner 1 with business partner 2 with business partner 1 being an organization.
Depending on the relationship type, choose whether the business partner is a person or an organization, and select the business partner roles that are permitted for each of the business partners in the relationship.
New values for Relationship Code must start with "Z".
Add Row
Remove
Relationship Code
Relationship Name
Relationship Description
Reverse Direction
Directional Relationship
Sales Area Dependency
Active
ZDIST
Distributor (Z)
Has a Distributor
Is The Distributor Of
ZMAIC1
ZPART
Pref. Svc. Contractor (Z)
Has Preferred Service Contractor
Is Preferred Service Contractor
ZPARTP
Pref. Svc. Cont. Per. (Z)
Has Preferred Sevice Contractor Person
Is Preferred Service Contractor Person
ZREL
Relationship Manager (Z)
Has a Relationship Manager
Is a Relationship Manager
Details: ZMAIC1 -
Business Partner 1
Organization:
Person:
Main:
Only One Relationship:
Allowed Roles
Contact:
Customer:
Prospect:
Sales and Service Partner:
Partner Contact:
Competitor:
Employee:
Service Agent:
Business Partner 2
Organization:
Person:
Allowed Roles
Contact:
Customer:
Prospect:
Sales and Service Partner:
Partner Contact:
Competitor:
Employee:
Service Agent:

3.7 System copy

If you do a system copy of one of your SAP Sales Cloud tenants, whether it is the QA tenant or the productive tenant, the following things must be respected:

Before the system copy:

- maiConnect must be deactivated for the target system in the AdminCockpit.

After the system copy:

- The maiConnect communication user must be checked in the copied system. Also whether the user has the required permissions (see chapter 3.3).
- The changed communication parameters must be updated in the AdminCockpit. This includes the tenant URL, the communication user and the password.
- The URL of the communication system must be adapted (see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**)
- The URL of the event notifications must be adapted (see chapter 3.5)
- It must be checked whether the users maintained in the AdminCockpit are still valid.
- Finally maiConnect can be reactivated via the AdminCockpit.